



N° 480

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

---

Enregistrée à la Présidence de l'Assemblée nationale le 6 décembre 2017.

## PROPOSITION DE RÉSOLUTION EUROPÉENNE

*sur le marché unique du numérique,*

(Renvoyée à la commission des Affaires économiques, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement)

PRÉSENTÉE,

AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES,

PAR M. ÉRIC BOTHOREL ET MME CONSTANCE LE GRIP,

Rapporteurs,



## PROPOSITION DE RÉSOLUTION EUROPÉENNE

### Article unique

- ① L'Assemblée nationale,
- ② Vu l'article 88-4 de la Constitution,
- ③ Vu les articles 16 et 114 du TFUE (Traité sur le fonctionnement de l'Union européenne),
- ④ Vu la directive n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,
- ⑤ Vu la directive n° 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;
- ⑥ Vu le règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),
- ⑦ Vu le règlement n° 526/2013 du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004,
- ⑧ Vu la Communication de la Commission européenne « Stratégie pour un marché unique numérique en Europe » du 6 mai 2015,
- ⑨ Vu la Communication de la Commission européenne « Créer une économie européenne fondée sur les données » du 10 janvier 2017,
- ⑩ Vu la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive

2002/58/CE (règlement « vie privée et communications électroniques ») du 10 janvier 2017,

- ⑪ Vu la proposition de règlement concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne du 13 septembre 2017,
- ⑫ Vu la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) du 13 septembre 2017,
- ⑬ Vu la communication de la Commission européenne « Un système d'imposition juste et efficace au sein de l'Union européenne pour le marché unique numérique » du 21 septembre 2017,
- ⑭ Considérant que la stratégie de la Commission européenne en faveur du Marché Unique du Numérique vise à favoriser la croissance d'un secteur dans lequel l'Union compte de nombreux atouts ;
- ⑮ Considérant que le potentiel de croissance dans le domaine de l'informatique en nuage pourrait atteindre environ 45 milliards d'euros en 2020 ;
- ⑯ Considérant la nécessité de mettre en œuvre le Règlement général sur la protection des données le 25 mai 2018 ;
- ⑰ Considérant que la protection des données de télécommunication est un complément nécessaire à la protection des données personnelles assurée par le Règlement général sur la protection des données ;
- ⑱ Considérant que la confidentialité des données personnelles doit être protégée, y compris en ce qui concerne les nouveaux acteurs de la télécommunication et ce, dans les différentes phases de collecte, de transfert, de traitement, de mise à disposition et de stockage des données ;

- ⑲ Considérant en particulier l'apport du chiffrement dit « de bout en bout » par rapport au chiffrement « de point en point » ;
- ⑳ Considérant qu'il est crucial que l'internaute puisse exprimer, en ce qui concerne les traceurs, un consentement éclairé, libre, spécifique et univoque, tel que défini par le Règlement général sur la protection des données ;
- ㉑ Considérant que la conservation des données sur des terminaux dans la durée doit demeurer une exception circonscrite par un cadre clairement défini et assuré par des mesures proportionnées ;
- ㉒ Considérant qu'il est vain, voire contre-productif, compte tenu des évolutions technologiques actuelles, de contraindre le stockage des données en fonction de considérations nationales ; considérant cependant que la localisation forcée de données peut répondre dans certains cas dûment justifiés à des questions de sécurité ou de difficulté d'accès aux données ;
- ㉓ Considérant que la libre circulation des données non-personnelles en Europe doit s'accompagner d'un principe de collaboration entre les autorités nationales des États membres ;
- ㉔ Considérant qu'il convient de faciliter la possibilité pour l'utilisateur de changer de fournisseur de service en nuage et la portabilité des données personnelles, à l'exclusion des données enrichies par le fournisseur du service ;
- ㉕ Considérant la nécessité de s'assurer de la qualité des produits échangés sur le marché unique du numérique ;
- ㉖ Considérant en particulier que la cybersécurité des produits doit être une priorité et que le degré de certification doit s'adapter à chaque type de produit, mais continuer à s'appuyer sur les standards de certains États membres, dont la France, qui figurent actuellement parmi les plus sécurisés au monde ;
- ㉗ Considérant la nécessité d'encourager tous les États membres à établir une politique publique de cybersécurité ambitieuse ;

- ⑳ Considérant qu'une telle politique ne peut s'appuyer que sur des organes publics ayant les moyens de répondre à des crises répétées mais aussi de diffuser les bonnes pratiques d'hygiène numérique, notamment ;
- ㉑ Considérant qu'une telle politique ne peut être menée actuellement que par les agences nationales, en coordination les unes avec les autres ainsi qu'avec l'ENISA ;
- ㉒ Considérant la nécessité de favoriser l'élaboration, avec les acteurs concernés, d'une doctrine civile d'emploi des technologies de l'information en matière de cybersécurité, dans le respect d'une éthique des entreprises et des principes fondamentaux qui régissent en Europe l'état de droit démocratique ;
- ㉓ Considérant la nécessité d'un système fiscal juste et efficace à l'échelle du marché unique du numérique, condition indispensable à une concurrence loyale entre les entreprises du secteur ;
- ㉔ Considérant le soutien que de nombreux États membres ont apporté à l'initiative française en faveur d'une taxe d'égalisation et l'agenda des travaux mis en place par la Commission européenne à ce sujet le 21 septembre 2017 ;
- ㉕ Considérant, que, selon l'Organisation de coopération et de développement économiques (OCDE), le modèle économique et certains attributs essentiels de l'économie numérique peuvent exacerber les risques d'érosion de la base d'imposition et de transfert des bénéfices ;
- ㉖ Considérant la volonté du Conseil européen de poursuivre la dynamique du chantier européen sur la fiscalité du numérique, en lien avec les travaux pour l'établissement d'une Assiette Commune Consolidée pour l'Impôt sur les Sociétés (ACCIS) ;
- ㉗ 1. Salue la poursuite de la stratégie pour un marché unique du numérique par la Commission européenne ;
- ㉘ 2. Soutient l'intégration des services de communication par contournement, également appelés « *over the top* », dans le

règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques ;

- ③7 3. Salue l'interdiction de stocker ou collecter des données sur des terminaux sans le consentement des utilisateurs ;
- ③8 4. Demande à ce que le consentement de l'utilisateur ne soit pas présumé en amont par le paramétrage automatique du navigateur mais à ce que ce consentement soit recueilli, notamment pour ce qui est des « *cookies* tiers », après une information claire de l'utilisateur ;
- ③9 5. Estime que l'adaptation de la législation française au Règlement général sur la protection des données doit viser une harmonisation maximale par le haut avec nos partenaires européens, afin de favoriser un cadre commun de protection des données personnelles ;
- ④0 6. Estime que les données relatives au trafic et les données de localisation ne peuvent être conservées par les autorités publiques que de manière proportionnée et à des fins expresses de sécurité et de défense nationale ;
- ④1 7. Souhaite garantir aux internautes leur droit d'exprimer le consentement libre, spécifique, éclairé et univoque au traitement des données ;
- ④2 8. Encourage le Gouvernement à supprimer tout obstacle potentiellement injustifié à la libre circulation des données non-personnelles au sein de l'Union européenne ;
- ④3 9. Souhaite qu'en complément de cette libre circulation soient mises en place des règles en matière de sécurité et de sûreté des données numériques, qui garantissent la transparence en ce qui concerne la localisation du stockage et du traitement de ces données ainsi que l'assistance mutuelle des autorités nationales pour faciliter l'accès aux données non personnelles stockées sur le territoire de l'Union européenne ;
- ④4 10. Encourage la création d'un droit à la portabilité des données non personnelles afin de permettre à tout individu ou

entreprise de récupérer les données générées par son utilisation d'un service et les transférer facilement auprès d'autres prestataires ;

- ④5 11. Considère que toute forme de certification des produits, et notamment des objets connectés, doit se faire de manière adaptée à chaque type de produit mais garantir à chaque fois un niveau ambitieux de protection ;
- ④6 12. Considère à ce titre que la sécurisation des produits doit être fonction de leur exposition au risque et de leur caractère stratégique, pour obéir à une approche proportionnée qui retiendra, selon le degré d'exigence, la solution la plus adéquate selon les niveaux de qualification ;
- ④7 13. Regrette dans ces conditions la faiblesse du système de certification prévu dans le « paquet » cybersécurité et demande à ce que les autorités nationales en charge de la cybersécurité demeurent, dans tous les États membres, les premières garantes de la protection des citoyens européens dans ce domaine ;
- ④8 14. Refuse dès lors que l'accroissement du mandat de l'ENISA, l'Agence européenne de cybersécurité, se fasse au détriment de l'action des agences nationales, ce qui pourrait aboutir à une diminution de la cybersécurité dans l'Union européenne ;
- ④9 15. Se réjouit de l'initiative française en faveur d'une taxe d'égalisation pour les acteurs du numérique ;
- ⑤0 16. Souligne que le secteur du numérique est particulièrement soumis aux stratégies non-coopératives aboutissant à l'érosion des bases fiscales et au transfert des bénéfices au sein de l'Union européenne ;
- ⑤1 17. Encourage le Gouvernement à appuyer les travaux de la Commission européenne et de la présidence du Conseil à ce sujet, en lien avec les travaux de l'OCDE, en vue d'un schéma de taxation équitable et d'une harmonisation des assiettes fiscales, tout en visant une harmonisation des taux d'imposition des services numériques ;

- ⑤② 18. Souhaite vivement que, dans le cadre de la proposition de directive sur le droit d'auteur dans le marché unique numérique, les plateformes participent à la juste rémunération des créateurs et à une lutte immédiate et efficace contre le piratage et la contrefaçon ;
- ⑤③ 19. Soutient les réflexions actuelles de la Commission européenne pour une responsabilité accrue des plateformes dans la lutte contre le contenu illicite en ligne.